Performance Work Statement
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)
Software Development Maintenance Services (SDMS)
Order ID: ID03180056006

1.0 INTRODUCTION

The Defense Manpower Data Center requires Software Development Maintenance Services (SDMS) to support the sustainment and maintenance of existing software applications, legacy systems, databases and interfaces.

2.0 BACKGROUND

Software sustainment is growing in importance as the inventory of DoD systems continues to age and greater emphasis is placed on efficiency and productivity in defense spending. A key mission for the DMDC is the development and maintenance of it applications, systems, databases and interfaces. Systems are increasingly reliant on software which must be sustained into the future. To sustain these systems organizations must define sustainment meet criteria to enter sustainment and overcome sustainment challenges.

While DoD Instruction 5000.02 describes sustainment in detail the Institute of Electrical and Electronics Engineers (IEEE) Standard Glossary of Software Engineering Terminology defines "software maintenance" as the process of modifying a software system after delivery to correct faults, improve performance or adapt it to a changed environment. It involves orchestrating the processes, practices, technical resources, information, and workforce competencies for systems and software engineering, to enable systems to continue mission operations and also to be enhanced to meet evolving threat and capability needs.

Sustaining software for the DoD, however, requires attention to certain issues (such as operations and training) that are less essential in commercial software maintenance. There are four primary categories of software sustainment activities:

- Corrective sustainment diagnoses and corrects software errors after release
- Perfective sustainment upgrades existing software to support new capabilities and functionality
- Adaptive sustainment modifies software to interface with changing environments
- Preventive sustainment modifies software to improve future maintainability or reliability

3.0 SCOPE

The scope of this work covers the full range of development and maintenance IT services to ensure uninterrupted service of existing applications, systems and related software; capturing user requirements; database administration; identifying functional, security, and performance requirements; providing design and program documentation, and supporting the Risk Management Framework (RMF) process.

4.0 OBJECTIVE

The objective of this task order is to identify and implement best commercial practices to modernize, streamline, centralize and standardize software development and sustainment in a more evolvable architecture that can better leverage state of the art computing capabilities in order to deliver the best available technology, reduce program sustainment costs, and maximize system reliability and performance.

5.0 PERFORMANCE REQUIREMENTS

The Contractor shall provide support for the tasks described below:

5.1 TASK 1 – PLANNING & MANAGEMENT OF SOFTWARE MAINTENANCE (FFP)

Tasks performed in support of this task order require management oversight, communications, time management, quality assurance and control, risk management, configuration management, cost management, and software integration. Using state-of-the-art knowledge, skills, tools, and techniques, the contractor shall:

5.1.1 Provide a Project Management Plan (PMP) that describes the proposed management approach, the milestones, tasks, and subtasks required by the task order. The PMP shall provide for an overall Work Breakdown Structure (WBS) and associated responsibilities. The Project Manager shall be responsible for a detailed PMP that identifies and assigns tasks, major milestones, dates and dependencies, and indications of critical path. The PMP shall include the status; statistics; risk management review; critical path; and other milestone progress checks and updates; as well as technical content review. The Government approved PMP will be used to monitor the Contractor's progress. The PMP is an evolutionary document, any revisions are considered incorporated upon written acceptance of the Government, inclusive of any changes to deliverables detailed in the PMP. The PMP shall be entered and maintained in Enterprise Project Server.

5.1.2 Provide information and recommendations to respond to Congressional, DOD, other Government agency, media or industry inquiries, Freedom of Information Act (FOIA) requests, audits and for Congressional testimony.

5.1.3 Maintain a real-time calendar of ongoing projects this includes maintaining, refining, and revising the project collaboration sites currently on SharePoint or other Government-designated repositories. This site must include project overview

documents, a consistently updated document library that preserves document history, schedules, a dashboard, assignment and POC lists, summaries and agenda for all meetings and conferences attended, and support for collaborative editing/versioning of project documents.

5.1.4 Coordinate with all impacted DMDC governance bodies such as DMDC Information Systems Security Group (DISSG), Architecture Review Board (ARB), Executive Governance Council (EGC), Enterprise Quality Assurance (QA), Configuration Management (CM), IT Operations, Consolidated Call Center (CCC), DMDC Management Advisory Group (DMAG), production support, implementation support, and other impacted divisions for project requirements and execution for approval authority.

5.1.5 Adhere to all DMDC Business Process Re-Engineering (BPR) workflows, requirements, and tool usage. Current BPR tools include Sparx Enterprise Architect, Microsoft Project Server, and Change Gear but could change throughout the life of this order.

5.1.6 Monitor legislative and policy changes; perform regulatory, legislative, policy and standards research and provide assessments to the government of impact to designated programs and IT products; and implement government directed legislative and policy changes.

5.1.7 Prepare ad-hoc white papers, information papers, point papers, presentations, briefings, business process assessments, and system assessments. Ad-hoc research requests to include performing special studies, conducting data research and respond to inquiries from DMDC customers.

5.2 TASK 2 – PERFORM SOFTWARE DEVELOPMENT MAINTENANCE SERVICES (SDMS) (TIME & MATERIAL)

Software sustainment involves orchestrating the processes, practices, technical resources, information, and workforce competencies for systems and software engineering, to enable systems to continue mission operations and also be enhanced to meet evolving threat and capability needs. Software sustainment activities can include correcting known flaws, adding new capabilities, updating existing software to run on new hardware and updating the software infrastructure to make software maintenance easier. The contractor shall perform all work using best software sustainment and commercial business practices, but not contradict Government business practices. Adhere to established software development standards and guidelines as prescribed by Capability Maturity Model (CMM), Capability Maturity Model Integration (CMMI), Institute of Electrical and Electronics Engineers (IEEE), and International Organization for Standardization (ISO) and DMDC Software Development instruction (Appendix B).

The Government will provide Application/Product Roadmaps (Appendix A) that detail the direction of the product and the work required to get there. The roadmap is used to

communicate the product direction and progress to internal teams and external stakeholders. Roadmap priorities shall be established by the Service Delivery Product Owner. Releases for the period of performance are reflected in the PWS and/or Appendix A. Releases listed on the Roadmap are estimated and scheduled within a calendar quarter but may be more frequent than quarterly. Additional quarterly releases will be managed based on DMDC priorities. The program requirements may vary from quarter to quarter but will not exceed the overall number of releases identified for the period of performance.

5.2.1 Support an agile development methodology (rapid development); software products shall be modular and reusable; sustain software capabilities in a manner that is responsive to immediate and future user needs.

5.2.2 Reduce and eliminate redundant tasks for sustainment efforts across all supported systems; e.g., develop software fixes in a manner that can be applied to multiple systems and consolidate management resources, functions, and tasks.

5.2.3 Create and update functional and technical specifications, design documentation, program specifications, unit test criteria, code and test program units, and produce program documentation.

5.2.4 Provide Tier Level 3 support (24/7/365) for application outages in production and data issues escalated by the Customer Contact Center (CCC), program manager, or application helpdesk.

5.2.5 Update applications and infrastructure in support of DMDC infrastructure improvements, changes, technical refreshes, or migrations (e.g., Common Update Framework (CUF), AION migration, Data Center location transition). Assist the government in converting and testing software to run on new hardware or virtualization platforms.

5.2.6 Develop and execute Software Test Plan(s) to address application or system use cases, user interfaces, security considerations, and reports using test data designed to demonstrate compliance with all documented functional specifications for each release.

5.2.7 Test software changes integrated with the existing software and/or other systems to verify that corrections and/or enhancements to software were successfully implemented and do not adversely affect any other components of the system or other systems.

5.2.8 Identify, plan, and conduct corrective, preventative, and adaptive maintenance

5.2.8.1 Perform corrective maintenance activities including the identification, isolation, and resolution of system problems to restore normal operations.

5.2.8.2 Perform preventative maintenance activities including systematic inspection, detection, and correction of problems before they occur to increase software maintainability and reliability, and to prevent problems in the future (e.g., applying application or operating system patches).

5.2.8.3 Schedule preventive maintenance, apply patches, and adhere to information assurance vulnerability alerts as well as planning for and management of multiple landscapes and transport paths and coordination across and support for multiple products/programs.

5.2.8.4 Perform adaptive maintenance activities designed to cope with changes in the software environment including the implementation of processing efficiencies, and/or considerations for additional delivered capabilities to enable existing and evolving requirements.

5.2.8.5 Implement methodologies and approaches to establish consistency in sustainment activities, develop preventive measures and document issue resolution procedures.

5.2.8.6 Provide day-to-day oversight of sustainment teams with emphasis on analysis, coding, testing, documentation, acceptance and maintenance phases.

5.2.8.7 Analyze root causes of operational malfunctions and coordinate resolutions, participate in escalated issues, address customer issues, and follow-up on outstanding issues.

5.2.8.8 Recommend process improvements to improve operational efficiency and develop standard operating procedures and knowledge base solutions.

5.2.8.9 Create and maintain a Software Maintenance and Development Plan (SMDP) that defines the approach, timeline and steps by which the development and maintenance of software applications will be accomplished and the management approach to software development and maintenance. The SMDP shall address software and sustainment processes, methods, organizational responsibilities, tools, configuration management, software quality, metrics, and other activities relevant to accomplish the requirements of the PWS. The plans shall be revised and updated as necessary to remain current and effective.

5.2.9 Application Information Security

5.2.9.1 Deliver software that meets the requirements of DoD and DMDC Information Assurance (IA) policy. Software shall be secure, accreditable and ensure security requirements are addressed in software design and development. Personnel performing IA activities shall obtain and remain current with, required technical and/or management certifications.

5.2.9.2 Ensure application code is updated with the latest security patches to minimize security vulnerabilities and provide documentation and confirm that application code changes comply with the DoD system security policy and are properly certified and accredited in accordance with current DODI 8510.01; Risk Management Framework (RMF) for DOD IT. Provide documentation as requested to support RMF Certification and Accreditation processes.

5.2.9.3 Implement procedural countermeasures and Government-issued technical advisories including Security Technical Implementation Guides (STIGs), service packs and security patches according to Automated System Security Incident Support Team (ASSIST) guidance within the timeframe specified by the technical advisory when such notices directly apply to the application software code used or developed. Report monthly completion of all Government issued technical advisories as described in this paragraph to the Information Assurance Officer.

5.2.9.4 Develop and implement a Software Security Risk Management Plan to assess and manage risk and coordinate with the Information Assurance Officer.

5.2.10 Unit Testing

5.2.10.1 Developers shall write unit tests to ensure that the unit (be it a method, class, or component) is operational and test across a range of valid and invalid inputs. In a continuous integration environment, unit tests shall be conducted anytime there a change to the source code repository.

5.2.10.2 Conduct a verification of the interaction one or more new or modified coded product components, as well as dependent components that have not been modified, to ensure complete coverage of requirements and successful interaction of components prior to full system testing.

5.2.10.3 Conduct interface (system-to-system), stress and volume testing, as part of development testing to identify issues as early as possible, reducing the risk and cost of rework.

5.2.10.4 Create test data in all testing environments.

5.2.10.5 Version and maintain all test artifacts in order to perform repeatable and reliable testing.

5.2.10.6 Develop test plans, data and tools that exercise the application at both the unit and systems integration levels.

5.2.10.7 Provide draft project artifacts to Enterprise Quality Assurance (QA) no later than two weeks prior to the anticipated QA start date; artifacts include: Requirements

Traceability Matrix (RTM), Functional Specifications, and Release Notes. The contractor shall revise QA release notes after submission, based upon unknown variables that emerge during development.

5.2.11 Release Management

5.2.11.1 Manage and plan all software releases; assess and manage risk and resolve issues that affect releases as they move forward. Communicate release details and schedules within fall DMDC environments. Continually work to make the release process better, faster and set a solid foundation that evolves.

5.2.11.2 Manage system software, hardware, and configurations, to include patches, emergency data fixes, and upgrades for each release. Inform system users of upcoming releases that will change or increase system functionality or capability.

5.2.11.3 Ensure each release is compliant with Risk Management Framework requirements to gain certification as required by DoD Information Assurance and DMDC policies. Ensure monthly Information Assurance Vulnerability Alerts (IAVA) issues are monitored and resolved. Coordinate new releases with stakeholders, hosting facility and owners of connected systems. Coordinate with and allow system access to the Government IA representative for routine testing and data collection as necessary or requested to comply with IA requirements to obtain or retain Authority to Operate.

5.2.11.4 Maintain a release log, build and release procedures, dependencies and notification lists.

5.2.12 Application Level Change Management

Manage and maintain the existing automated software build and deployment infrastructure for each deployed application in support of the following environments: stand-alone workstations, Local Area Network/Wide Area Network (LAN/WAN) development, LAN/WAN Test, and LAN/WAN Quality Assurance (QA). This includes but is not limited to overseeing the source code repository, infrastructure, common library components, and scripts required to perform CM automation. Coordinate with DMDC Release Planning to monitor, coordinate and stage required artifacts for each scheduled release. Software shall be staged based on scheduled and out of-cycle release planning in support of the following environments. The environments may include the following: stand-alone workstations, LAN/WAN networks, Contractor Test, Stress Test and Production. Government review and approval is required prior to promoting to production environments. Provide a pre-deployment checklist to ensure all software is accounted for in each release and process change requests managed through the DMDC Configuration Management infrastructure.

5.2.13 Configuration Management (CM)

5.2.13.1 Develop and maintain a configuration management plan (CMP) that tracks and controls changes in software to include revision control and the establishment of baselines. The CMP is a dynamic document, and shall be updated as work proceeds and the necessity arises.

5.2.13.2 Identify, define and baseline configuration items (CI)

5.2.13.3 Control modifications and releases of CIs; record status of Cis and any modifications ensuring consistency and completeness

5.2.14 Production Support

5.2.14.1 Monitor process and software changes that impact production support, communicate project information to the production support staff and raise production support issues to the product owner. Support scheduled and unscheduled, on-request and end-user initiated processing of business applications.

5.2.14.2 Maintain a run log for all batch applications. Implement procedures for proactively identifying, preventing, and responding to problems. Provide ongoing running and monitoring of batch systems, such as the personnel data feeds, Security, Point in Time and Database Extract.

5.2.14.3 Maintain and support all Test, Model Office, user acceptance test, benchmark test, stress test, and Production regions, including systems and applications components Support updates and monthly loads of address validation software.

5.2.14.4 Develop and maintain Disaster Recovery Activity (DRA) and Continuity of Operations (COOP) plans for every required application and interface.

5.2.14.5 Provide escalation support to understand, troubleshoot, root cause, log analysis and resolve complex technical issues.

5.2.14.6 Provide daily support with resolution of escalated tickets and act as liaison to product and technical leads to ensure issues are resolved in timely manner. Communicate with source of escalation, complete appropriate documentation, and process tickets according to agency methodology.

5.2.15 Requirements Traceability Matrix (RTM)

Create or update Requirements Traceability Matrix for all projects/products. The RTM shall clearly link the new and/or changed requirements to where and how they have been implemented in the system. The RTM shall provide backwards and forward traceability

documenting each requirement from its source through definition, analysis, design, testing, acceptance, and deployment.

5.2.16 Cyber-Security & Information Assurance (IA)

5.2.16.1 Ensure that all system or application deliverables meet the requirements of DoD and DMDC Information Assurance (IA) policy and that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications. Protect system information and resources according to established security policies and procedures and ensure application code is updated with the latest security patches to minimize security vulnerabilities.

5.2.16.2 Provide documentation and confirm that application code changes comply with the DoD system security policy and are properly certified and accredited in accordance with DODI 8510.01; Risk Management Framework (RMF) for DOD IT, signed 12 Mar 2014. The Contractor shall be consistent with established disciplines and best practices for effective systems engineering, systems security engineering, and program protection planning outlined in DoDI 5000.02.

5.2.16.3 Provide documentation to support RMF Certification and Accreditation processes. Final approval for all IA tasks under this contract belongs to the Information Assurance Officer, Cyber Security Branch. The contractor shall obtain final approval for all IA-related design decisions, including cryptography, authentication, access control, data transfer and storage, Need-to-Know (NTK), or other IA technologies that must be coordinated with and approved by Cyber Security Officer.

5.2.16.4 Identify potential program, system, and engineering risks that pertain to cyber security; and participate in and support the development of risk mitigation plans and monitoring of risk mitigation activities.

5.3 TASK 3 – CONDUCT BUSINESS REQUIREMENTS ANALYSIS (FFP)

Business requirements analysis is a comprehensive declaration of what the project is supposed to achieve and a step-by-step procedure to discover, analyze, and document the essential requirements connected to the product. Business analysis involves frequent communication with system users to determine specific feature expectations, resolution of conflict or ambiguity in requirements defined by the various users, avoidance of feature creep and Identification of possible technical solutions and best value alternatives.

5.3.1 Conduct requirements analysis, feasibility, migration, business process reengineering, requirements validation through interaction with functional proponent, requirements traceability, business process modeling, rules, data requirements, and interface management. Document workflow, business processes, data and services, and include a

standard set of artifacts for the purpose of understanding the program asset/software requirements.

5.3.2 Collaborate with stakeholders to formulate and communicate requirements; prepare a business requirements document (BRD) that details the solution documenting customer needs and expectations. Conduct requirements and design walkthroughs with external and internal consumers.

5.3.3 Translate requirements to design modifications maintaining the integrity of the product's design, develop user scenarios and interfaces.

5.3.4 Provide business process-improvement support that includes all activities involved in helping improve customer data systems through business processes including rethinking program design and aligning information technology infrastructures with business missions, goals, and objectives.

5.3.5 Create data flow diagrams, perform data standardization and perform enterprise modeling, functional economic analysis, simulation/modeling, activity based costing and activity based management support.

5.3.6 Provide "as is "and "to-be" functional analysis.

5.3.7 Software and Systems Integration & Implementation

5.3.7.1 Facilitate and monitor the integration, interoperability, and synchronization of enterprise-wide systems and infrastructure solutions and services.

5.3.7.2 Develop a systems integration plan to oversee the development of external dependent projects and provide a strategy for the successful integration of all software and hardware into the environment. Plan to include roles and responsibilities, assumptions, internal and external stakeholders, integration/coordination with external organizations, implementation schedules and status, interdependencies of applications, systems integration, design review and acceptance procedures and schedules, user acceptance testing support, privacy and security management (site security, data privacy/security), and defect tracking and resolution.

5.3.8 Software Transition Support

The Contractor shall provide support for transition of the delivered software components to the Government or Government-specified Contractor, to include, but not be limited to, performing software test and verification, training, and corresponding documents that provide information on the use and maintenance of the software and its components. The Contractor shall prepare a project specific Software Transition Plan. The Software Transition Plan shall address products to be turned over (documentation, software, hardware, tools), formats and media, schedules,

and support during transition. The Contractor shall include all resources needed to control, copy, and distribute the software and its documentation. The Contractor shall identify at the Test Readiness Review all hardware and software that will be transitioned during each delivery and the time frame of the transition.

5.4 TASK 4 – CONDUCT DATA QUALITY MANAGEMENT (DQM) (FFP)

Data Quality Management in the DoD is essential to mission success. It ensures that quality data supports effective decision making and that the correct data gets to the right person at the right time. DMDC requires Data Quality Management that incorporates a cycle in which continuous observation and improvement leads to improvement in the quality of data assets across the enterprise. Data quality management responsibilities fall under the DoD information management and data administration initiatives (DODD 8000.1 and DODD 8320.1).

Conduct data quality assessment using data profiling to identify the degree to which poor data quality impedes business objectives and prepare a DQ assessment report

5.4.1 Define business related data quality and validity rules; perform measurements and set performance targets

5.4.2 Design quality management processes that remediate process flaws

5.4.3 Inspect, monitor and remediate when quality of data is not acceptable.

5.4.4 Automate data quality with tools such as:

- edit checks
- reports
- automation of functions to evaluate quality of data

5.4.5 Produce a Data Quality Implementation Plan that establishes processes and procedures in line with DoD and organization goals.

5.4.6 Provide a means to identify, track, and report non-conforming data and recommendations on preventive and corrective actions to improve data quality.

5.4.7 Provide a monthly report of the status of data quality and produce metrics indicating the quality of data.

5.4.8 Provide data cleansing efforts that correct existing data quality issues and improve future data quality.

5.4.9 Research and analyze on TASS and PDR data discrepancies from the monthly data pull reports.

5.4.10 Benefits Error Analysis

The Government estimates the volume of daily personnel transaction files to include 10 active duty files per day; 14 Reserve Components Common Personnel Data System (RCCPDS) files per day; up to 10 Guard Reserve Initial Duty (GRID) files per day (Reserve/Guard components do not send a file every day); and 7 Guard Reserve Active Service (GRAS) Analysis Report files daily.

5.4.10.1 Review daily transactions rejected in the batch processes with primary focus on Personnel Finance Transfer (PFT), GRAS, and GRID to include handling rejects, documenting fixes and tracking volumes. Correct not less than an average of 100 errors daily and complete the following actions:

- Determine root cause and appropriate response
- Coordinate with the service liaisons
- Make recommendations for corrective actions

5.4.11 Medical Satellite (MedSat) and Person Data Repository (PDR) Benefits

5.4.11.1 Develop internal data quality scripts that produce high quality data leading up to the data conversion activities; the government estimates 30 errors per day that require intervention.

5.4.11.2 Ensure all data discrepancies that would negatively impact the data conversion are resolved; it is expected there are less than 10 categories of errors that will negatively impact the data conversion activities.

5.4.11.3 Analyze and resolve data discrepancies and anomalies identified through internal quality control monitoring.

5.4.11.4 Review and update data conversion scripts, correspondence, carry forward drive time waivers; correct handling of PCM assignments, and region changes.

5.5 TASK 5 - OPERATE The Common Access Card (CAC) Central Issuance Facility (CIF) (FFP)

The Common Access Card CIF is the Department of Defense's (DoD) enterprise solution for bulk production and issuance of CAC cards and their PINs for more than 200,000 new recruits and other DoD personnel annually by collecting required demographic and identity information, processing that data to produce the cards centrally, and shipping the cards to pre-determined locations including eight basic training sites, three academy sites, and two officer training schools.

5.5.1 Operate and maintain the CIF Pre/Post Process Server (PPS) Client Software which drives the creation and printing of the CAC Cards including:

- Process bulk submission requests and data.
- Process cards for encoding.
- Load CAC holder certificates onto the card.
- Load CAC holder photo and other standard biometric information onto the card.
- Set the card's PIN.

- Print the card.
- Seal the card in the DMDC approved confidential packaging for shipping.
- Ship the card to the CAC holder at the designated location.
- Print the PIN and seal it in a confidential mailer from a separate physical location.
- Ship the confidential mailer containing the PIN to the CAC holder at the designated location, in accordance with DoD and DMDC guidelines.

5.5.2 Deliver CACs and PINs to the designated location within timeframes listed in the chart below. There shall be zero deviations from the Service Level Agreements (SLA) with the customers and all deviations will be coordinated with the customer location once it is known that the SLA will not be met. All shipments shall be made using the Government shipping account. All shipments shall be made using the most cost-effective shipment method that will still meet the delivery SLA.

Service/Site	Timeframe
Army	Next business day for CACs and no later than two business days for PINs
Marine Corp	No later than five business days for CACs and no later than five business days for PINs
Navy, Air Force & Service Academies	No later than three business days for CACs and no later than three business days for PINs

5.5.3 Provide a monthly CIF Operations Report that provides SLA deviations, explanations for the deviation, remediation actions and actions taken to prevent future deviations. Report shall also include total CAC production, issues, risk and remediation.

5.5.4 Perform maintenance and updates to the CIF environment, printers and all CIF components following DOD and DMDC procedures.

5.5.5 Coordinate with Enterprise Quality Assurance to conduct test runs and changes utilizing the CIF test environment and the bulk printing components. Verify the results.

5.5.6 Maintain physical control of smartcard stock and other consumables present in the CIF; ensure physical and logical access controls to the Secure CIF environment are followed.

5.5.7 Document all issues using the DMDC approved tool for prioritization and scheduling

5.5.8 Collaborate and provide support to CIF vendors and stakeholders.

5.5.9 Conduct maintenance, integration, installation and testing and diagnostic support of the CAC Infrastructure components
- Profile Studio/Profile Manager (PS/PM)
- Key Management System (KMS)
- Inventory Logistics System (ILS)
- Card Content Server (CCS)
- Exchange Manager (EM)

5.5.10 Maintain, update and operate the User Portal (CCS, 4tress Profile Manager/Profile Studio) on the Issuance Portal and Post Issuance Portal and the Inventory Logistics System Non-classified Internet Protocol (IP) Router Network (NIPRNet) tokens.

5.5.11 Support the RAPIDS CAC infrastructure, incidents and outages and CAC components (CCS, KMS, ILS, PS/PM & EM) 24x7x365. Support services include Production and Disaster Recovery Regions Support (24x7x365) in all TEST, MODEL and Production environments.

5.5.12 Include all defects and issues in the Monthly Status Report (MSR). Historically there have been 0 - 5 SRT calls per month per Credentialing/Identity Management applications.

5.5.13 Maintain valid production encryption keys used in TEST, MODEL, Production and Disaster Recovery environments through the operation of the Key Management System.

5.5.14 Perform security patching, analyze and mitigate Information Assurance Vulnerability Alerts (IAVA).

5.5.15 CAC Testing Support (OPTIONAL) (TIME & MATERIAL)

The DoD Test Common Access Card Request (TCR) is used to obtain test CACs to assist in the development of applications. RAPIDS issues test CACs and Alternate Logon Token Issuance & Management System (ATIMS) for issuance of Alternate Logon token request. All new identities shall be created in the test instance of Defense Enrollment Eligibility Reporting System (DEERS). The contractor is responsible for packaging and shipment of the test tokens. Shipments shall be recorded and logged.

5.6 TASK 6 – SUPPORT THE NON-COMBATANT EVACUATION OPERATIONS TRACKING SYSTEM (NTS) & EMERGENCY TRACKING ACCOUNTABILITY SYSTEM (ETAS) (FFP)

The Government estimates six (6) major software releases annually

5.6.1 Sustain and enhance NTS/ETAS applications including online and offline capabilities (Appendix A); integrate new technologies and requirements from the NTS/ETAS user community. Conform to DMDC mandated technology and ensure the system in is compliance within the required timeline.

5.6.2 Remediate vulnerabilities and security findings in production and update Plan of Action and Milestones (POA&M) to capture how the determination was addressed.

5.6.3 Evaluate and test new and existing hardware (e.g. scanners, printers, tablets, and webcams) and software with test cases to ensure full functionality. Integrate hardware and ensure legacy hardware continues to function with each release. Estimate level of effort for integration for Government approval.

5.6.4 Demo the NTS/ETAS software to the Government product owner and Service Delivery Branch Chief before releasing to Enterprise QA.

5.6.5 Conduct troubleshooting of the NTS/ETAS web application in development and production.

5.6.6 Assist and provide expertise with audits and data calls.

5.6.7 Travel and participate in DoD exercises twice a year to OCONUS/CONUS locations.

5.6.8 Provide Tier III support for hardware, software, database analysis, data quality issues and configuration outages across all DMDC deployment regions.

5.6.9 Update and maintain currency of the NTS artifacts and User Guide based on customer and DMDC feedback

5.6.10 Develop the capability to remotely deliver software installation files to a permanent locations so NTS POCs have constant file access.

5.6.11 Research new software and hardware technologies that provide solutions to problem sets, determine feasibility of integrating into the application, and estimate the level of effort for integration into NTS/ETAS.

5.6.12 Coordinate with DoD and federal agency partners requesting access to the NTS system and reports.

5.6.13 Maintain and update the NTS Information website.

5.7 TASK 7 - Enhance and Sustain the Automated Central Tumor Registry System (ACTUR) (OPTIONAL) FFP

ACTUR is a tri-service application, which collects and reports on data from Army, Air Force, and Navy facilities. The ACTUR application is currently used at over one hundred Military Treatment Facilities (MTFs) throughout the U.S., Europe, and the Far East. The main goal of ACTUR is to provide appropriate information to numerous cancer research organizations, like the American College of Surgeons (ACoS) Commission on Cancer (CoC) that utilize the National Cancer Database (NCDB).

The user base consists of roughly 120 users worldwide and the application is responsible for about 4,000 transactions per day. ACTUR includes the ACTUR Manager, ACTUR Web Application, and ACTUR Reports.

5.7.1 Provide an ACTUR Project Management Plan (PMP) that identifies and assigns tasks, major milestones, dates, dependencies and indications of critical path. The PMP will include the status; statistics; risk management review; critical path; and other milestone progress checks and updates; as well as technical content review. Tasks from the final and Government approved PMP shall be selected as milestones against which Contractors' progress shall be monitored. The PMP is an evolutionary document that shall be updated annually and identify tasks and deliverables specified in operating procedures that shall be completed by the contractor. Any updates to the PMP shall be incorporated to the task order upon Government approval.

5.7.2 Provide end-user support for problems or defects with ACTUR products

5.7.3 ACTUR REPORTING

5.7.3.1 Develop, maintain, and implement quality control procedures for ad-hoc and recurring data requests and reports. Produce the following reports:

- National Cancer Database (NCDB) report
- North American Association of Central Cancer Registries (NAACCR) cancer report
- Ad-Hoc state agency reports
- Rapid Quality Reporting System (RQRS) to Army, Navy and Air Force

5.7.3.2 Conduct twice- weekly "NCDB Data Pull"

5.7.3.3 Migrate ACTUR Reports from COGNOS to SAS

5.7.3.4 Attend the Monthly ACTUR User Group Meetings

5.7.3.5 Provide the Center for Cancer Research (CCR) data reports

5.7.3.6 Provide a monthly activity/status report that includes the following:

- Complete & Incomplete Case Status Report
- Data Submission Report
- Data Sub-report

5.7.3.7 Conduct Site Security Management (SSM) provisioning new users in both ACTUR Web and the ACTUR Reporting tool.

5.7.4 Conduct ACTUR SW Sustainment & Enhancements

5.7.4.1 Conduct all phases of software maintenance as defined in ISO/IEC 14764. Possible categories are corrective maintenance, adaptive maintenance, perfective maintenance, and preventive maintenance.

5.7.4.2 Add, modify, and delete functionality based on customer requirements.

5.7.4.3 Conduct quarterly maintenance releases that include security updates to the application.

5.7.4.4 Implement procedures for proactively identifying, preventing, and responding to problems.

5.8 TASK 8 – SPECIFIC SUSTAINMENT REQUIREMENTS (FFP)

This section relates to the specific products and applies to the applications as a group.

5.8.1 Sustain and enhance the Real-Time Automated Identification System (RAPIDS) Application Suite - (The Government anticipates 4 major releases annually) See Appendix A for products and release data.

5.8.1.1 Migrate RAPIDS to WebLogic 12c.

5.8.1.2 Conduct a technology refresh of RAPIDS dependent components (Java, ActivClient middleware, PDF form viewer).

5.8.1.3 Remediate and execute tasks identified on the product owner prioritized list for JIRA maintenance.

5.8.1.4 Integrate next model camera with Aware PreFace.

5.8.1.5 Sustain and maintain the use of Probabilistic Search in RAPIDS.

5.8.1.6 Support the development and testing for implementation of the DoD Next Gen USID card.

5.8.1.7 Develop and test requirements for Foreign Affiliate Lockdown and surrogate additions; support DS Logon transition from Security Online to EMMA for user provisioning.

5.8.1.8 Sustain and enhance RAPIDS applications; integrate new technologies and requirements from the RAPIDS user community.

5.8.1.9 Evaluate and test new and existing hardware (e.g. scanners, printers, tablets, and webcams) and software with current test cases to ensure full functionality. Integrate hardware and ensure legacy hardware continues to function with each release. Estimate level of effort for integration.

5.8.1.10 CAC Pin Reset

5.8.1.10.1 Migrate to WebLogic 12c.

5.8.1.10.2 Conduct a technology refresh on dependent components (CCS 5, Java, ActivClient middleware, PDF form viewer).

5.8.1.10.3 Configuration Management Tool.

5.8.1.10.4 Conduct bug remediation and resolve urgent updates with each RAPIDS release.

5.8.1.10.5 Sustain and document the Satellite Access Service (DSAS) applications.

5.8.1.10.6 Migrate Message of the Day to WebLogic 12c.

5.8.1.10.7 Sustain and enhance Rapids Logon Monitor (RLM) application.

5.8.2 Trusted Associated Sponsorship System (TASS) - (4 Major releases annually)

5.8.2.1 Conduct research, analysis, and troubleshooting to resolve production issues.

5.8.2.2 Support enterprise software & hardware; complete development tasks to support DMDC Enterprise software and hardware changes, includes but not limited to new hardware, software migrations.

5.8.2.3 Complete development tasks associated with high and medium priority backlog JIRA tickets.

5.8.2.4 Conduct bug remediation and resolve urgent updates of the Verifying Official Information System (VOIS) with each RAPIDS release.

5.8.3 Infrastructure Support - (4 Major releases annually)

5.8.3.1 Conduct bug remediation of the Audit server and resolve urgent updates with each major release of RAPIDS.

5.8.3.2 Migrate Bulk Certificate Revocation to WebLogic 12c.

5.8.3.3 Support, develop and test the Web Based Bulk Revocation (WBBR) interface.

5.8.3.4 Sustain the Token Issuance Infrastructure.

5.8.3.5 Transition functionality of Site Maintenance Tool (SMT) to ID Card Office Online (IDCO) 3.0 and migrate to WebLogic 12c. The Government estimates two (2) releases annually.

5.8.4 Application Security Suite (FFP) reference Appendix A for roadmap and product list- (The Government estimates 4 Major releases and 4 Minor releases annually)

5.8.4.1 Sustain and enhance Application Security Suite (appendix A) applications; integrate new technologies and requirements. Conform to DMDC mandated technology and ensure the system in is compliance within the required timeline.

5.8.4.2 Enterprise Management & Monitoring of Accounts (EMMA) Web User Interface (UI) Framework.

5.8.4.3 Migrate Enterprise Management & Monitoring of Accounts (EMMA) Web User Interface Angular.

5.8.4.4 Update ASIS/COAL to require a valid DoD PIV authorization certificate at logon by January 31, 2020 as per DOD CIO memo 'Modernizing the Common Access Card – Streamlining Identity and Improving Operational Interoperability' dated December 7, 2018.

5.8.4.5 Conduct bug remediation and resolve urgent updates with each security suite release.

5.8.4.6 Modify EMMA web site to include search functionality.

5.8.4.7 Monitor and respond to JIRA tickets submitted to its queue. There were a total of 511 tickets submitted during the last 12 months.

Ticket Action	Timeframe
Triaged/assigned (100%	Within 2 Business Days
Resolved (90%)	Within 10 Business Days
Escalated	If ticket cannot be resolved within 10 business days, it will be escalated to government lead.

5.8.5 **Defense Enrollment Eligibility Reporting System (DEERS)** - Conduct all phases of software maintenance as defined in ISO/IEC 14764. Possible categories are corrective maintenance, adaptive maintenance, perfective maintenance, and preventive maintenance for all applications and products in accordance with Appendix A. The major subsections are:

5.8.5.1 **Veterans Affairs Benefits (Education & VLER) releases)**

5.8.5.2 **Benefits & Entitlements**

5.8.5.3 **Infrastructure Support**

5.8.5.4 **TRICARE Enrollment**

5.8.5.5 **TRICARE Eligibility & Claims**

5.8.6 Identity Web Services (IWS) Suite of Applications

5.8.6.1 Sustain and enhance Internet Web Services Suite of Applications (Appendix A); integrate new technologies and requirements. Conform to DMDC mandated technology and ensure the system in is compliance within the required timeline.

5.8.7 Provide HID SME support in support of HID products used in the RAPIDS Suite.

5.9 **TASK 9 – CONDUCT FACIAL RECOGNITION ANALYSIS (OPTIONAL) FFP**
The Government anticipates four (4) releases annually

Provide program management support to include support of a facial recognition Office. Assist the Government in the planning, implementation, maintenance, and operation of the Facial Recognition Software Automation Implementation capability.

5.9.1 Analyze Facial Recognition data utilizing DMDC data. The contractor shall consult with DMDC stakeholders for requirements. The analysis shall consist of:

- Analysis of specifications and programming approaches
- Analysis of incoming data to ensure compliance with technical specifications and quality standards for various initiatives
- Collaboration with data submitters to manage all facial recognition requests
- Communicate corrections and recommend remediation to improve requests for proper submittal/acceptance by DMDC

5.9.2 Respond to Facial Recognition requests from customers within 10 days of receiving the request. Manage the data request through DMDC Data Request System (DMDCRS) and provide monthly analyze of the number requests received.

5.9.3 Conduct business analysis and post-production release support; communicate with software vendor on bug analysis, correction, verification and implementation, performance metrics and standard operation procedures.

5.9.4 Document application architecture.

5.10 TASK 10 – AUTOMATE FACIAL RECOGNITION (OPTIONAL) (TIME & MATERIAL)

5.10.1 Conduct the system and integration activities such as requirements, design, development and internal development testing for TacID software and scope future enhancements for application automation.

5.10.2 Produce a technical design to specify the technical architecture, technical functionality; user interfaces and interfaces as required by the application automation phase of the product.

5.10.3 Prepare and execute milestone reviews for requirements, design, development and testing as required by the DMDC lead, to ensure the development meets the needs of the Government. The milestones shall be outlined in the government approved project management plan.

5.10.4 Update the COTS product into DMDC's infrastructure.

5.10.5 Assist in documentation of the application architecture for the DMDC Architecture Repository.

5.10.6 Provide documentation for functional and technical specifications, data quality reviews, mission security assessments and mission impact assessments; Investigate, prepare and execute milestone reviews for requirements, design, development and testing.

5.10.7 Analyze specifications, formulate programming approaches, and consult with DMDC and its customers to clarify requirements.

5.10.8 Analyze incoming data to ensure compliance with the required technical specifications and quality standards for various initiatives.

5.10.9 Collaborate with data submitters to manage all data intake. Communicate corrections and recommend any remediation to improve the data analytical value.

5.11 TASK 11 Common Update Framework (CUF) (FFP)

5.11.1 CUF (Four major releases)

5.11.2 Sustain and maintain CUF, conduct all phases of software maintenance as defined in ISO/IEC 14764. Possible categories are corrective maintenance, adaptive maintenance, perfective maintenance, and preventive maintenance.

5.11.3 Continue the work on CORE to CUF migration, work with all CUF client applications to migrate them to the new data access processor being modified within 6-months of the new processor being deployed to production.

5.11.4 Separate the CUF-EJB application into two separate components—one component for the web service and one component for the CUF dashboard.

6.0 TASK 12 – PROVIDE PLANS, REPORTS, AND DOCUMENTATION (FFP)

6.1 Monthly Status Report (MSR) and Senior Management Reviews (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ

6.2 Meeting Summaries

The Contractor shall follow the Meeting Summaries requirements identified in the PWS Section 5.8.4 of the EITS II Base IDIQ

6.3 Weekly In-Progress Review (IPR)

The Contractor shall follow the IPR requirements identified in the PWS Section 5.8.5 of the EITS II Base IDIQ

6.4 Problem Notification Report (PNR)

The Contractor shall follow the PNR requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ

6.5 Expenditure Resources Report

6.5.1 Provide an Expenditure and Resource Report (ERR) to the DMDC COR on a monthly basis. The Contractor shall submit the quarterly ERR by the twenty-fifth (25th) calendar day of the month after the end of the month for services rendered. This report shall be detailed by each project/product that is being worked by the contractor in support of this PWS, the amount that will be billed to the Government and the resources (hours and personnel) assigned to that task. Each report shall provide the current month and cumulative task order costs breakout as a monthly subset by project organized by line item, with a total at the end of the row for the particular application/product/project.

6.5.2 The report shall link all products related to a specific application, with a roll up on the total cost for a particular application if applicable. (For example RAPIDS as a top line and all products that are part of RAPIDS linked to RAPIDS showing a total effort for

RAPIDS suite of applications, Facial Recognition on the other hand would stand alone since there are no other products lined to that application).

6.5.3 The report shall separate sustainment costs from enhancement costs, and organized by line item.

6.5.4 The report shall separate FFP from time and material costs and be organized by line item.

6.6 ORIENTATION/POST AWARD CONFERENCE

The Contractor shall follow the Orientation/Post Award requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ

6.7 **DELIVERABLES**

The Contractor shall submit a draft version of each deliverable and the government will provide written acceptance, comments and/or change requests, if any, in accordance with PWS Section 7.0. The Contractor shall make any corrections and submit the final deliverable to the contractor established and maintained approved site location (currently Sharepoint), in accordance with the dates listed in the following table and in accordance with PWS Section 7.0:

PWS Section	Deliverables	Date Due/Frequency
5.1.1	Project Management Plan (PMP)	Draft submitted within 20 work days of order award; Final submitted within ten days after receipt of Government comments. Updates as needed and no less frequently than 30 days after exercise of an Option Period.
5.1.3	Maintain SharePoint Site	Updated 5 days after award and updated within 2 days after documents change
5.1.3	Project Documentation	30 days after award and updated within 2 days after documents change
5.1.4	DMDC Governance approvals	Per Government approved PMP
5.2.8.9	Software Maintenance Development Plan (SMDP)	• Draft due within 30 days of contract award • Final due IAW Inspection and Acceptance clause • Updated monthly
5.2.9.4	SW Security Risk Management Plan	20 days after award
5.2.10.6	Test Plans	Per Government Approved PMP
5.2.13.1	Product Configuration Management Plan	30 days after award and
5.2.15	Requirements Traceability Matrix (RTM)	Per Government Approved PMP

5.3.2	Business Requirements Document	Per Government Approved PMP
5.5.2	CAC/PIN Delivery	Per Section 5.5.2 of the PWS
5.5.3	CAC CIF Report	Monthly
5.6.1	Online/Offline Solution	Per government approved Implementation Plan
5.6.9	Update documentation and knowledgebase artifacts	Within 60 days of award, and in conjunction with each release
5.6.10	Remote SW Installation Files	Per government approved Implementation Plan
5.6.11	NTS/ETAS Implementation Plan	Within 30 days of award
5.7.1	ACTUR Project Management Plan	15 days after award
5.7.3.1 5.7.3.5 5.7.3.6	ACTUR Reporting • NCDB Report • NAACCR Report • State Reports • RQRS Service Report • NCDB Data Pull • CCR Data Report • Monthly Activity Report	 Annually Annually Ad-Hoc Monthly Bi-Weekly As Requested Monthly
5.7.3.3	Migrate ACTUR reports from COGNOS to SAS	Per Government approved ACTUR PMP
6.1	Monthly Status Report/Senior Management Review	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
6.2	Meeting Summaries	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
6.3	Weekly In-Progress Review (IPR)	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
6.4	Problem Notification Report (PNR)	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
6.5	Expenditures Resources Report	NLT 25th of each month
6.6	Post Award Orientation	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
6.7	Final deliverable posted to approved location	Posted no later than deliverable due date
6.8	Quality Control Plan	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
8.0	Non-Disclosure Agreement	Prior to any contractor personnel reporting for work
11.3	Tele-work Agreement	Prior to any telework

6.8 Quality Control Plan (QCP)

The Contractor shall follow the QCP requirements identified in the PWS Section 5.9.1 of the EITS II Base IDIQ

6.9 Quality Assurance

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.10 of the EITS II Base IDIQ

7.0 PERFORMANCE STANDARDS

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

Performance Objective	PWS Paragraph	Performance Threshold	Method of Surveillance
Analysis, design, development and maintenance tasks shall be completed on time in accordance with approved project schedule		Maintain 90% accuracy and timeliness	Periodic (Quarterly)
Work, with limited direction, stays on schedule, on cost, and in scope typically responsible for independently defining approach to tasks and solutions to problems		Meet all government performance, schedule and cost requirements with 95% compliance	Periodic (Monthly)
Unscheduled application downtime		Contractor restores application within 48 hours	COR/TPOC monthly review of system metrics
Scheduled application downtime		Equal or fewer than 12 hours	COR/TPOC monthly review of system metrics
Mean Time To Restore		Time allowed for the system to be offline	COR/TPOC monthly

(MTTR)		after application availability is interrupted. Mission-critical IT systems (RAPIDS, Application Security, IWS and DEERS) have a MTTR of two hours or fewer; non-mission-critical IT systems (all others) have a MTTR as short as five hours	review of system metrics
User incidents		(X affected users / Y total users) * 100 = % Application Availability; Maximum % effected dependent on mission criticality	COR/TPOC monthly review of system metrics
Release and Production Drop Schedules		Bugs and defects found in production will not force a rollback 75% of the time	Schedules reviewed at the Weekly IPR
Software Management		98% of scheduled upgrades and/or maintenance are executed according to schedule For non-mission critical applications, 90% of requests for unscheduled software maintenance are responded to within 48 hours For mission critical applications, 100% of requests are responded to within 2 hours	Event Driven and activity reports
Application & System Security Compliance		Maintain 100% application security compliance IAW applicable DoD policy and instruction, DoD Instruction 8500.2 – Information Assurance particularly the Security Technical Implementation Guide (STIG)	100% inspection
Develop and maintain up-to-date user documentation		100% compliance to Create/Maintain/deliver to government, documentation of all code, to include user help files. Develop and maintain up-to-date digital and hard copy user documentation for framework applications to include user guides, administrator guides, tutorials, and online help within 5 days of release.	Routine Inspection of Deliverable Products/Services
Perform Vulnerability management		Category 1 (CAT I) vulnerabilities eliminated within 24 hours of identification of a vulnerability or the contractor must provide a get well plan approved by the government.	Routine Inspection as Products /Services are submitted
Adherence to Schedule		Contractor meets TO delivery requirements 100% of the time. Unless	Inspection of Deliverable

		there is a prior approval from the DMDC COR.	Products/Services
High Quality Technical Performance *Performance meets all technical and functional requirements, and is highly responsive to changes in technical direction and/or the technical support environment* *Deliverable reports contain all required data and meet all requirements*		Contractor delivery of products and/or services meets all TO requirements. Performance occurs with no required re-work at least 95% of time. Problems that are encountered are minor and resolved in a satisfactory manner.	Routine Inspection of Deliverable Products/Services

8.0 Non-Disclosure Requirements

The Contractor shall follow the Non-Disclosure requirements identified in the PWS Section 8.6 of the EITS II Base IDIQ.

9.0 Cooperation with Other On-Site Contractors

The Contractor shall follow the Cooperation with Other On-Site Contractors requirements identified in the PWS Section 11.7 of the EITS II Base IDIQ.

10.0 KEY PERSONNEL

The contractor shall designate and identify contractor employees who will be considered key to operations for efforts under this task order. These key personnel must have an in-depth understanding of the requirements and their responsibilities as well as the ability, knowledge, experience, and skills to perform the requirements. They shall be fully committed to the success of the mission. The contractor shall designate key personnel for the following tasks:

- Program/Project Manager
- Senior Software Engineer (SSE)
- Information Assurance Manager

11.0 Contract Administration.

This Task Order shall follow all of the requirements identified in the EITS II IDIQ.

11.1 Contract Type: Firm Fixed Price (FFP) and Time and Material (T&M)

11.2 Period of Performance: The period of performance for this Task Order shall be 12 months from date of award with two one year options.

11.3 Place of Performance/Hours of Operation: At least 50% of the work under this task will be performed on site at DMDC facilities in Seaside, CA. The remaining percentage of work may be performed at a contractor provided facility. Any work performed at other locations must be identified in the formal submission and approved by the Government. Occasional travel may also be required, as noted in PWS Section 11.6- Travel. If the contractor anticipates personnel will telework, they shall identify a plan to COR for acceptance.

The contractor is responsible for conducting business between the hours of 8 a.m. to 5p.m depending on their physical location. Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

11.4 Post Award Conference: The Contractor shall follow the IPR requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ.

11.5 Points of Contact:
DMDC COR
Will be assigned Post Award

GSA Contracting Officer (CO)
Mr. Ryan Schrank
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: ryan.schrank@gsa.gov
Tel: 215-446-2853

GSA Contract Specialist (CS)
Mr. Mike Levey
GSA-FAS, Mid-Atlantic Region

The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Mike.Levy@gsa.gov
Tel: 215-446-5806

GSA Contracting Officer's Representative (COR)
Mr. Scott Ostrow
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Scott.ostrow@gsa.gov
Tel: 215-446-4497

11.6 Government Furnished Property/Equipment/Information (GFP/GFE/GFI): The Contractor shall follow the requirements identified in the PWS Section 10.8 of the EITS II Base IDIQ.

11.7 Travel: The cost reimbursable not-to-exceed travel limit is estimated at $10,000.00 per year. It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs.

Before contractor travel is executed, authorization must be given by the COR.
All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

11.8 Security: The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ.

12.0 Inspection, Acceptance, and Payment:

The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this contract. The designated officials are responsible for inspection and acceptance of all services, incoming shipments, documents and services.

The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

13.0 APPENDICES

Appendix A – Software Development Roadmap
Appendix B – Automation Standard Best Practices
Appendix C – Enterprise QA Roles and Responsibilities
Appendix D – DMDC ARB Charter References (Enclosure 1)
Appendix E – DMDC ARB Charter Required Artifacts (Enclosure 2)
Appendix F – DMDC ARB Charter Process Map and Description (Enclosure 3)
Appendix G – DMDC ARB Charter
Appendix H – CEAS Project Charter
Appendix I – CEAS Reports List
Appendix J – Template Checklist
Appendix O – EHRM Applications